ENGLISH TRANSLATION

OF INTERNATIONAL APPLICATION

PCT/EP02/01382

(12) INTERNATIONAL APPLICATION PUBLISHED IN ACCORDANCE WITH THE PATENT CO-OPERATION TREATY (PCT)

(19)World Intellectual Property Organization
International Office

[WIPO logo]

[bar code]

(43) Date of International Publication:
August 22, 2002 (8/22/2002)

PCT

(10) International Publication Number:
WO 02/065403 A1

(51) International Patent Classification[7] : G07C 9/00

(21) International Appl. No.: PCT / EP02/01382

(22) Filed: February 9, 2002 (2/9/2002)

(25) Language submitted in: German

(26) Language published in: German

(30) Priority Data
101 06 956.1 February 15, 2001 (2/15/2001) DE
101 38 014.3 August 2, 2001 (8/2/2001) DE

(71) Applicants *(for all designated states except the US)*: **LEOPOLD KOSTAL GMBH & CO. KG** [DE/DE] ; Patent Department, Wiesenstrasse 47, 58507 Lüdenscheid (DE).

(72) Inventors; and
(75) Inventors/Applicants *(only for US)*:
Eduard BERGMANN [DE/DE]; Im Langen Hahn 34, 58515 Lüdenscheid (DE). **Armin VON PREETZMANN** [DE/DE]; Strassburger Allee 63, 44577 Castrop-Rauxel (DE).

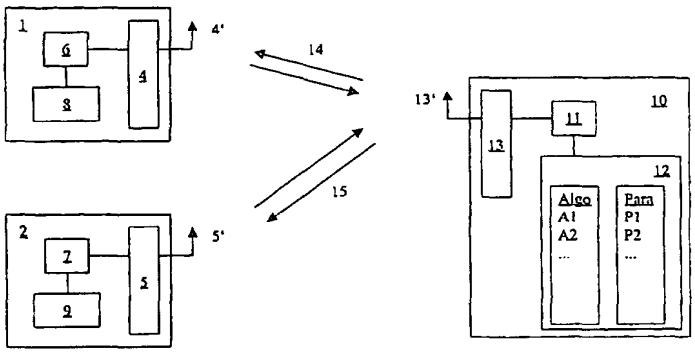
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
— *With an international research report*
— *Before the deadline which applies for changes to claims; will be republished if changes are made.*

For explanation of the two-letter codes and other abbreviations, please see the section entitled "Guidance Notes on Codes and Abbreviations" at the beginning of every regular edition of the PCT gazette

(54) Title: KEYLESS ACCESS CONTROL DEVICE



(57) Abstract: The invention relates to a keyless access control device that comprises at least two object modules with transmitter/receiver devices associated with a given object, and one or more identification providers that comprise at least one microprocessor each. Data are exchanged via a bi-directional data communication path between the identification provider(s) and the object modules. Said data are encoded by means of an encryption algorithm and an symmetrical encryption method that uses encryption parameters that are associated with the respective object module. The inventive device is substantially more flexible for the adaptation to changing boundary conditions as compared to conventional devices since it uses from the start at least two different encryption algorithms.

Keyless Authorized Access Control Device

Description

This invention concerns a keyless authorized access control device with at least two object modules, each of which is assigned to a certain object and each of which comprises transceivers, and with one or more identification devices, each having at least one microprocessor, with all of the identification device(s) and object modules having a bidirectional data communications link between them that can transfer data, which is encoded by means of an encryption algorithm and a symmetric encryption method using encryption parameters assigned to the respective object module.

The invention also concerns an identification device and an object module for such a keyless authorized access control device.

Keyless authorized access control devices are used where controlling access by means of a mechanical key is not desired. For example, such authorized access control devices are used in motor vehicles and in the area of the house. The intended opening of the respective object, for example the motor vehicle or the house, is done by the wireless transfer of a corresponding command together with an encoded record (called "code" for short) from an identification device that is carried by a user to a transceiver that is assigned to each desired object. If the transceiver associated with an object receives the code belonging to the object, the person carrying the identification device is considered to be authorized to have access, so that access is then enabled by triggering certain actuators to unlock the motor vehicle, for example. In order to make it unnecessary to carry several identification devices when several keyless authorized access control devices are used, identification devices and corresponding authorized access control devices have been developed which allow a single identification device to be used for an authorized access control query with several objects, for example the motor vehicle, the house, and possibly the work place.

The previously known devices, which allow authorized access control to be performed for several objects using a single identification device, work according to the principle that all objects' transceivers work with the same encryption algorithm. Such devices are disclosed in DE 195 33 309 A1 and DE 196 07 017 C2, for example.

The object of DE 195 33 309 A1 involves composing the code that is transferred of a fixed code and a changing code, both of which are sent together to open a motor vehicle. When such an authorized access control device is used, in order for it also to be possible to give identification devices to persons who may only open the house, however not the motor vehicle, this authorized access control device has one or more other identification devices which transmit only one code: the changing code.

The object of DE 196 07 017 C2 involves transferring data between each identification device and the transceivers assigned to the objects over a bidirectional data communications link, with the data being encoded by means of a symmetric encryption method. When this is done, the transferred data is encoded by means of an encryption algorithm that is used to perform the symmetric encryption method using certain encryption parameters, each of which is a so-called encryption secret assigned to the addressed object. This device provides an adjustment of the encryption parameters between identification devices and the respective object in a so-called learning mode.

A common characteristic of these known authorized access control or identification devices is that they use one and the same encryption algorithm for authorized access to different objects. The resulting low flexibility is a disadvantage, especially for objects which have a different life expectancy, such as a motor vehicle and a house, for example. When one of the two objects is changed, it is not absolutely guaranteed that the new object which is added will work with the same encryption algorithm, so that the object module associated with the remaining object will probably also have to be changed. Especially when the number of objects is even greater, conflict is almost unavoidable when one of the objects is changed or when another object or identification device is added.

By contrast, the device according to the invention is clearly more flexible at adapting to changing conditions, since from the start it allows the use of at least two different encryption algorithms; in a first embodiment this capability is provided in the identification device, and in a second embodiment it is provided in at least one of the object modules (preferably in the one with the longest service life, such as a house, for example). This makes it possible, for example in the first embodiment when an object is changed, to select another encryption algorithm in the identification device for the new object module, or, if necessary, to replace an old encryption algorithm with a new one by reprogramming the identification device, without this affecting the other encryption algorithms implemented in the remaining object modules. The second embodiment is especially advantageous in the case when the former vehicle is replaced by a new one, for example, and thus at the same time the identification device belonging to the old vehicle is replaced by a new one, which works with a different encryption algorithm than the old one. In this case, if the encryption algorithm used by the new identification device is already present in the memory element of the other object module, e.g. that of the house, this encryption algorithm is activated for this identification device; otherwise it is stored in place of the old encryption algorithm that is no longer needed by reprogramming, without this interfering with other encryption algorithms affecting other identification devices.

The invention is described below using a sample embodiment which refers to the attached figures.

The figures are as follows:

Figure 1: A schematic illustration of a first embodiment of a keyless authorized access control device according to the invention;

Figure 2: An alternative to the identification device shown in Figure 1.

In a keyless authorized access control device, an identification device 10 gives a user authorized access to several objects. The identification device 10 shown in Figure 1 contains the necessary means of electric transmission and reception 13 to communicate with transceivers 4, 5 of the object modules 1, 2 assigned to the respective objects, and thus to be able to exchange encoded data via bidirectional data communication links 14, 15 to establish authorized access. When this is done, the data is encoded both in identification device 10 and in object modules 1, 2 by microprocessors 11, 6, 7 using a symmetric encryption method, with identification device 10 and each addressed object module 1, 2 using the same encryption parameters P1, P2 to encrypt the data. These encryption parameters represent the encryption secret between the identification device 10 and each of the object modules 1, 2. The identification device 10 has a separate set of encryption parameters P1, P2 for each object module 1, 2 stored in a memory element 12; these encryption parameters differ from one another. Each of these sets of encryption parameters P1, P2 can be changed, in a known manner in coordination with both sides, during the course of a data exchange between the

identification device 10 and the object module 1, 2 which uses the respective set of parameters, in order to prevent the encryption secret being found out by spying. In addition to encryption parameters P1, P2, identification device 10 also has stored in memory element 12 various encryption algorithms A1, A2, ... that are suitable for carrying out a symmetric encryption method and are commonly used, with each object module 1, 2 having a fixed encryption algorithm assigned to it, which is the one that the respective object module 1, 2 also uses itself. The fixed assignment of the encryption algorithm for the identification device to use in reference to the respective object module occurs, so to speak, when the two devices "become acquainted" by a single initialization process. In contrast to encryption parameters P1, P2, the currently valid form of each of which is characteristic for the respective object module 1, 2, the encryption algorithms used by the object modules 1, 2 do not necessarily differ from one another. Thus it is entirely possible, e.g., for several object modules 1, 2, 3, ..., to use one and the same algorithm, perhaps A1, for example, while only a single object module N uses a different algorithm A2, or similar combinations. What is decisive is that identification device 10 has a number of commonly used algorithms A1, A2, ... stored in it, which can be called up by microprocessor 11 if they are needed, e.g., if a new object module is added. From the stock of encryption algorithms A1, A2, ..., which are located in memory element 12 of the identification device 10, it is also possible for individual, unnecessary algorithms to be replaced by newer ones through a programming interface, without this affecting the algorithms that are still necessary for other object modules.

The alternative identification device 10 shown in Figure 2 differs from the one shown in Figure 1 in that here instead of only a single microprocessor 11 it provides for the use of two independent microprocessors 11 and 11', each of which has its memory elements 12 and 12' directly integrated into it. Of course, such integration of a memory element 12 in the microprocessor 11 is also possible in the identification device 10 shown in Figure 1. However, the design shown in Figure 2 has the advantage over it that the second microprocessor 11', with the additional algorithms stored in its memory 12', is hardware which is also completely exchangeable, if necessary, so that reprogramming is unnecessary even when an algorithm is supposed to be used which has not yet been provided for use. By contrast, the first microprocessor 11 with its memory 12 remains in identification device 10, so that its operation in connection with the object module(s) that are still being used is not affected by the exchange.

While the first embodiment of the keyless authorized access control device according to the invention which has been described up to here assumes a universal identification device, so to speak, which can cooperate with several object modules using different encryption algorithms, a second embodiment provides that at least one universal object module is present, which, for its part, can cooperate with several identification devices using different encryption algorithms. Of course, in a maximal configuration it is also possible to use both a universal identification device and universal object modules simultaneously.

Claims

1. Keyless authorized access control device with at least two object modules (1,2), each of which is assigned to a certain object and each of which comprises transceivers (4,5), and with one or more identification devices (10), each having at least one microprocessor (11, 11'), with all of the identification device(s) (10) and object modules (1, 2) having a bidirectional data communications link (14, 15) between them that can transfer data, which is encoded by means of an encryption algorithm and a symmetric encryption method using encryption parameters (P1, P2) assigned to the respective object module (1, 2), **characterized by the fact** that a (the) memory element(s) (12, 12') present in the identification device(s) (10) have a total of two or more different encryption algorithms (A1, A2, ...) stored in them, which the microprocessor(s) (11, 11') can selectively call up in relation to each object module (1, 2) that is addressed.

2. Authorized access control device according to Claim 1, characterized by the fact that the encryption algorithm (A1, A2,...) to use is assigned to the respective object module (1, 2) by a single initialization process.

3. Keyless authorized access control device with at least two object modules (1,2), each of which is assigned to a certain object and each of which comprises transceivers, and with one or more identification devices (10), with all of the identification device(s) (10) and object modules (1, 2) having a bidirectional data communications link (14, 15) between them that can transfer data, which is encoded by means of an encryption algorithm and a symmetric encryption method using encryption parameters (P1, P2) assigned to the respective object module (1, 2), **characterized by the fact** that a memory element (8, 9) present in at least one object module (1, 2) has two or more different encryption algorithms (A1, A2, ...) stored in it, with it being possible in each case to establish the encryption algorithm to be used in relation to the identification device (10) that is used.

4. Authorized access control device according to Claim 3, characterized by the fact that the encryption algorithm to be used is assigned to the respective identification device (10) by a single initialization process.

5. Identification device for a keyless authorized access control device for exchanging data with object modules (1,2) assigned to objects and comprising transceivers (4,5), with the data being encoded in a microprocessor (11, 11') by means of an encryption algorithm and a symmetric encryption method using encryption parameters (P1, P2) assigned to the respective object module (1, 2), **characterized by the fact** that a (the) memory element(s) (12, 12') have a total of two or more different encryption algorithms (A1, A2, ...) stored in them, which the microprocessor(s) (11, 11') can selectively call up in relation to each object module (1, 2) that is addressed.

6. Identification device according to Claim 5, **characterized by the fact** that at least the encryption algorithms (A1, A2) stored in one memory element (12, 12') can be manipulated and/or replaced through a programming interface.

7. Identification device according to Claim 5 or 6, **characterized by the fact** that at least one memory element (12, 12') is integrated in an assigned microprocessor (11, 11').

8. Object module for a keyless authorized access control device with a transceiver (4, 5) for exchanging data with an identification device (10), with the data being encoded by means of an encryption algorithm and a symmetric encryption method using encryption parameters (P1, P2) assigned to the object module, **characterized by the fact** that a memory element (8,

9) has two or more different encryption algorithms (A1, A2, ...) stored in it, with it being possible to establish the encryption algorithm to be used in relation to each identification device (10) that is used.

9. Object module according to Claim 8, **characterized by the fact** that the encryption algorithms (A1, A2, ...) stored in the memory element (8, 9) can be manipulated and/or replaced through a programming interface.

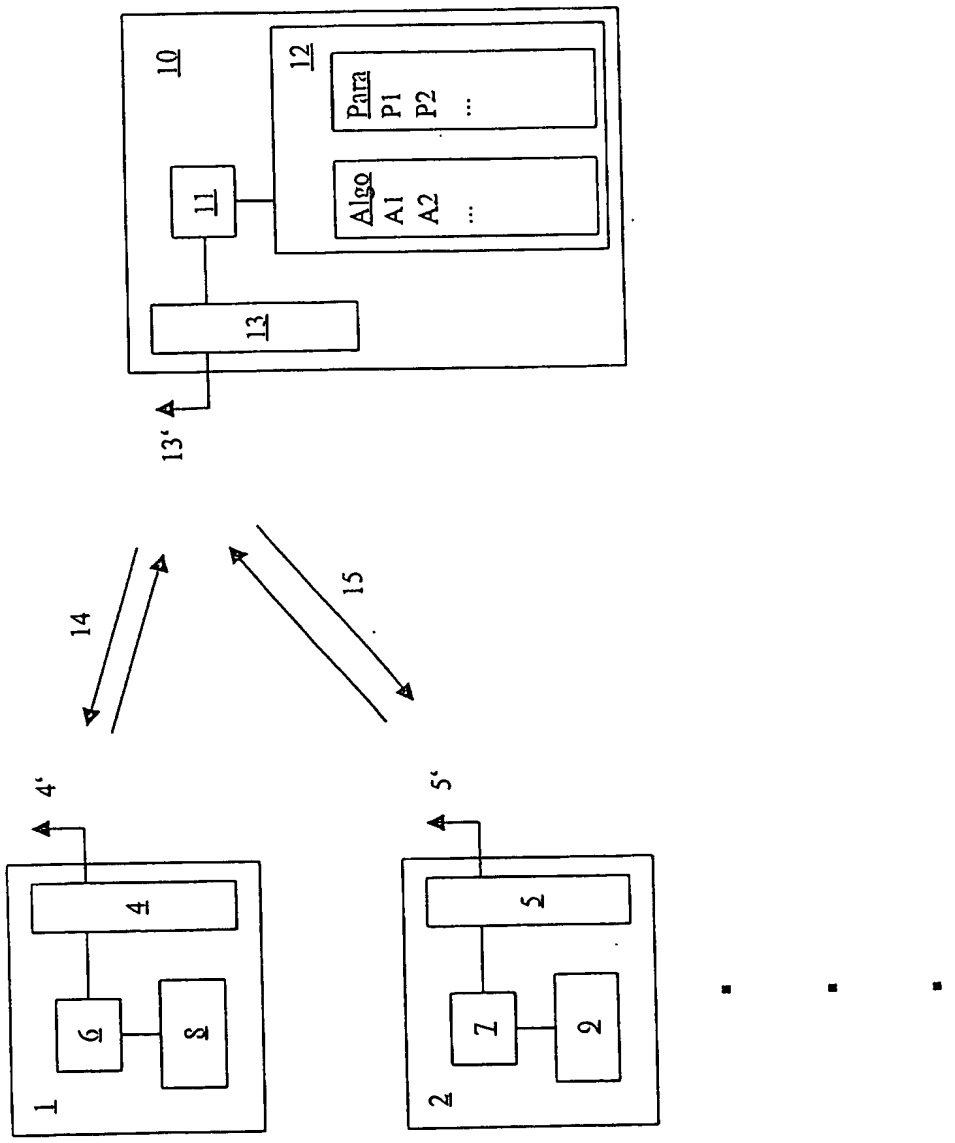


Fig. 1

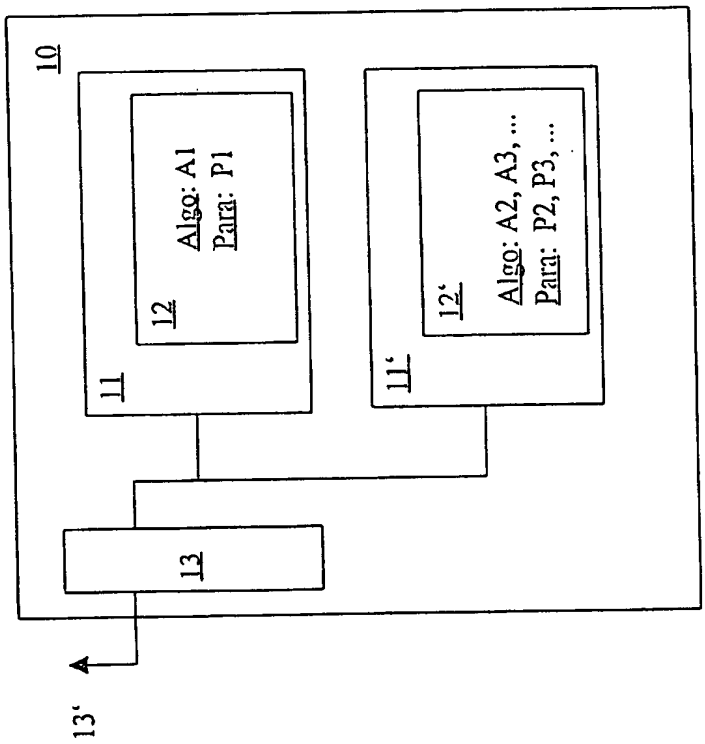


Fig. 2